STATEMENT BY

TERESA M. TAKAI
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON

EMERGING THREATS AND CAPABILITIES

ON

FISCAL YEAR 2013 BUDGET REQUEST FOR

INFORMATION TECHNOLOGY AND CYBER OPERATIONS PROGRAMS

March 20, 2012

NOT FOR PUBLICATION UNTIL RELEASED BY THE SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES, HOUSE ARMED SERVICES COMMITTEE

Introduction

Good afternoon Mr. Chairman and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee on the importance of information technology (IT) to the transformation of the Department of Defense (DoD). I am Teri Takai, and I am the Department's Chief Information Officer (CIO). My office is responsible for leading the Department's information enterprise and ensuring that DoD is as effective and efficient as possible by ensuring that the right information is available to the right people at the right time and the right place. I am responsible for ensuring that DoD information and information technologies can be depended upon in the face of threats by a capable adversary. To do all this in a place as large and complex as the Department clearly requires that DoD information technology be done as a team across all Department organizations. I would like to give you an overview of some important DoD information technologies, technical efforts in cybersecurity, and provide an update on the Department's IT modernization efforts currently underway.

Overview

The Department's FY13 IT budget request of approximately $37 billion includes funding for a broad range of information technology, including: desktop computers, tactical radios, identity management technology, human resource systems, commercial satellite communications, financial management systems, and much more. These investments support mission critical operations that must be delivered in both an office environment and at the tactical edge on the battlefield. These investments provide capabilities that enable the Commander-in-Chief to communicate with and direct the military, support intelligence activities as well as logistics, medical and other business support functions of the Department. The Department's IT environment is even more complex when one considers that these investments operate in over 6,000 locations worldwide, support the unique needs and missions of the three Military Departments and over 40 Defense Agencies and Field Activities within the Department. The Department's IT budget request represents a slight decrease from the FY12 IT budget. This decrease represents savings associated with initial IT effectiveness and efficiency efforts identified by the DoD Components. I anticipate additional savings as the Department implements some of the actions I will describe below. Included in the overall IT budget is approximately $3.4 billion for defensive cybersecurity efforts that are designed to ensure our

information, information systems and networks are protected against known cyber vulnerabilities and are resilient to ever-increasing cyber threats the Department and the nation face. This portion of the IT budget has not decreased and continues to receive the highest-level attention and support of the Department.

DoD's Information Environment

The scale of the Department's networks is illustrative of the complexity of the Department's information infrastructure and IT budget. The networks reach almost every corner of the globe and connect active duty, reserve and national guard as well as civilians and our contractor support base totaling roughly 3.7 million people with active cyber identity credentials issued by the DoD public key infrastructure, or PKI. These credentials are contained on the DoD's common access card, or CAC, and allow each of these people to access the Department's unclassified network and its rich information sharing capabilities. The Department has approximately 25,000 servers that are visible to the Internet, and countless people from DoD's partners access DoD information resources every day and exchange information with DoD personnel.

Information technology is changing rapidly, and DoD is accelerating its efforts to take advantage of the operational, efficiency, and possible cybersecurity improvements of these changes. As an example, we have broad piloting of advanced commercial mobile technologies in every Military Service, and I expect to approve broader deployment of smart phones and tablet computing for unclassified use within the next several months. The Defense Information Systems Agency (DISA) and the National Security Agency (NSA), are working together with industry and have developed security configuration baselines for several of the major smart phone technologies and are working on more. To enable the agile deployment of new and innovative applications to these devices while preserving vital cybersecurity, we are also piloting application storefronts that will be used to manage the configuration of these many devices, and will also be used as a place from which to download new secure applications.

Joint Information Environment

In August 2010, the Secretary directed a number of initiatives to achieve savings in acquisition, sustainment, and manpower costs, while not degrading the Department's ability to execute its missions. Among these is the consolidation of the Department's IT infrastructure, while simultaneously defending that infrastructure against growing cyber threats. Planners from throughout the Department put together a set of initiatives and in the Fall of 2011, the Deputy Secretary signed out the IT Enterprise Strategy and Roadmap (ITESR).

I am currently leading the implementation of this effort, teamed with the Joint Staff along with the Services and many other DoD organizations, to more aggressively modernize the Department's overall information environment. Our primary goals are to make the Department more effective and more secure against cyber threats and vulnerabilities. A secondary, but very important goal is to reduce the cost associated with the Department's overall information technology infrastructure by simplifying, standardizing, centralizing, and automating infrastructure at the enterprise level. We are calling the result of the effort the Joint Information Environment, or JIE. We are using the intelligence community's information technology modernization efforts to inform much of the JIE planning. A team consisting of experts from throughout DoD is currently fleshing out the approach and is developing an implementation plan of action and milestones, and cost estimates.

In addition to benefits for end-users and cyber defenders, the JIE will speed up capability deployment, while making new capabilities easier to defend and more secure. In today's DoD IT environment, a typical IT program develops and integrates the entire IT "stack", which includes the network, the computers, the standard software loads on the computers, and the core machine-to-machine services like messaging, and global load balancing. In addition, the program must integrate cybersecurity across all of this, from operating system configuration, to access controls, to perimeter defenses, to cyber intrusion detection and diagnosis. Today, this effort is replicated for almost every IT program because of the disparate infrastructures and architectures that have evolved in DoD.

In contrast, the JIE will provide program offices an integrated "platform" of network computing, core enterprise services, and security. In many, if not most cases, program managers will be able to build on top of all or a substantial part of this standard platform. With much of the work already done, programs will deliver faster, and will inherit better cybersecurity from the start. Via efforts like DISA's Forge.mil and RACE software development environments, and via integrated test and security evaluation capabilities that match the production platform, we believe we can also help speed up the development, and the quality control and cybersecurity evaluations for programs.

Network Consolidation

One of the central pillars of the JIE is to restructure the Department's networks so as to move DoD to a single, joint network architecture for each security level. For the unclassified network, this is enabled by our new enterprise perimeter defenses. We are currently developing the engineering and architecture details of this JIE element. The goal is to repurpose many of the current, organization-unique perimeter defenses into standard, joint, regional perimeter defenses that will be shared by all DoD organizations within a particular geographic region, and that will all be managed to common operational policies set by Cyber Command. This will provide much more uniform cyber defenses, will allow Cyber Command to be able to "see to the desktops" and will help keep successful intrusions from spreading within the networks, and will improve interoperability and dependability for joint missions.

Data Center Consolidation

The restructuring of the Department's networks will be done in conjunction with data center consolidation. Currently, DoD has an excess of capacity in data centers. The DoD CIO, in coordination with the Services and Defense Agencies, will set standards for the type and design of these data centers. The standards will be essentially identical for the unclassified network (NIPRNET), secret-classified network (SIPRNET), and any cryptographically and/or physically separate mission networks the Department constructs. This consolidation, in conjunction with the move to more enterprise information services, will allow the Department over time to significantly reduce the number of data centers from the more than 770 data centers identified in

our 2011 inventory. By the end of fiscal year 2012 DoD will reduce its inventory of data centers by more than 115.

The objective of this effort is to consolidate DoD existing data centers into three types of standard data centers. Core data centers will be used for information services and applications that must be available broadly across DoD, and for the Department's outward-facing applications and services required for interaction with industry and the public. These will in fact become the initial DoD cloud computing instantiation. We also anticipate establishing regional data centers that will host information services and applications that are better placed closer to end-users in the region. Examples include print servers, thin client servers, and servers that control access to end-user devices. Finally, we also envision the possibility for some forward deployed/deployable data centers. The centers will be flexible and will hold both regional and enterprise services and data, all tailored to the mission situation and to the speed and reliability of the connection to the more fixed portions of the network.

The servers in these computing centers will generally be highly virtualized so as to allow agile insertion of new information services, to provide portability of applications, data, and eventually whole data centers between regions, and to provide maximum efficiency. Like the layout of the enterprise computing centers themselves, the layout of the server virtualization in the enterprise computing centers will be done in accordance with the existing DoD CIO cybersecurity engineering standards and the applicable DoD Security Technical Implementation Guides for server virtualization, for perimeter defenses, and other technologies.

One other significant improvement in this new data center and network structure will be the standardization of the technology for the remote operation of the defenses, the network, the data centers, the servers, and the applications, so as to significantly improve the cybersecurity of the Department's IT control systems. This remote management will be done in accordance with the DoD data center standard, and the applicable cybersecurity standards.

Commodity Purchasing

The Department has achieved cost avoidance estimated at over $3 billion over a 10 year period through our Enterprise Software Initiative (ESI). DoD organizations have achieved significant efficiencies in the purchase of software, hardware and services from the open market. This is achieved as a result of terms and conditions negotiated with vendors whose products appear in the ESI inventory. Our IT Enterprise Strategy and Roadmap emphasizes the increased use of commodity purchasing of hardware, software, and services as a major means of achieving efficiencies. Through the sharing of purchase agreements across organizations within the Department, we are able to minimize the number of purchase vehicles in use, further streamlining our IT acquisition processes.

Enterprise Services & IT Governance

Many commonly used information technology services can be more effectively, securely, and efficiently provided "from the cloud", which means from the core data centers. This centralization can reduce staff, but by centralizing, can ensure the operations and defense staffs are more highly trained and practiced. We are moving more aggressively to enforce the use of common applications and services, like email, web collaboration, search, file storage, video, and voice over IP. The successful web conferencing service called Defense Connect On-line is an early example.

To make this vision of a true enterprise approach to the DoD's information technology work, I am also working with other senior leaders at the Pentagon to ensure that governance of IT investments is viewed at an enterprise level and enables agile delivery of it capabilities and solutions, consistent with authority provided by Congress in the FY10 National Defense Authorization Act under Section 804.

Additionally, we are working to resolve some of the cultural, structural, and other challenges in migrating to enterprise solutions. For example, we believe that the "Cloud First" strategy developed by the Office of Management and Budget (OMB) as part of the 25 Point Implementation Plan to Reform Federal Information Technology Management is a promising approach towards consolidating IT and reducing duplicative IT applications. We have developed

a draft cloud strategy for the Department and will be working hard with the Military Departments, DISA, other Components and industry to implement cloud approaches to better optimize our IT infrastructure and applications in the near future.

The above efforts are all ongoing and being aggressively worked across the Department. In leading these efforts, my office has worked very closely with the Military Department CIOs and had some early successes. Notable examples of this include extensive collaboration with Army, Air Force and DISA to establish an implementation approach for DoD Enterprise Email – an important step toward true enterprise solutions. Similarly, my office is working closely with the Navy and the Under Secretary of Defense for Acquisition, Technology and Logistics as the Navy and Marine Corps transition from Navy Marine Corps Intranet (NMCI) to the Next Generation Enterprise Network, to ensure enterprise-wide and cybersecurity issues are addressed in the release of the Request for Proposal.

The result of these consolidation initiatives will be a DoD Joint Information Environment that provides the warfighter with the required access to information and services needed to accomplish their mission from any location with any device and that are dependable in the face of cyber threats by a capable adversary. This standardized information and network infrastructure will eliminate the organizational barriers to information sharing and eliminate seams which malicious actors can exploit to gain access to vital information or systems. It will also increase the flexibility of defense networks to incorporate or respond to changes in emerging technology by minimizing the disparity within the Department's information architecture.

Cybersecurity

As noted above, the $37 billion of the IT budget includes approximately $3.4 billion for DoD's cybersecurity program. This includes funding for cybersecurity practices, processes, technologies, and operations throughout the Department. Virtually every DoD mission depends on the Department's information infrastructure. These missions often depend on the information and information infrastructures of our mission partners and industry.

The Department exercises leadership of its cyber activities through a close relationship of several Department organizations. In my capacity as the DoD CIO, I am responsible for the information assurance and defense of the Department's information networks and systems. I provide guidance and oversight regarding the day-to-day defense and protection of DoD information networks and systems; IT support to military and joint missions; resilience and reliability of information and communication networks; and overall policy and guidance for the Department's IT investments. I work closely with the Under Secretary of Defense for Policy, and specifically the Assistant Secretary of Defense for Global Strategic Affairs, who is responsible for developing Department's overall cyber strategy and policy. General Alexander, as Commander of Cyber Command is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department's information networks and when directed, conducts full-spectrum military cyberspace operations (in accordance with all applicable laws and regulations) in order to ensure U.S. and allies freedom of action in cyberspace, while denying the same to our adversaries.

We have five primary goals for the department's cybersecurity efforts. The first goal is that customers of the DoD information infrastructure, including the Department's mission partners, can depend on essential information and information infrastructure in the face of cyber warfare by a capable adversary. The DoD's operational environment will always contain cyber threats, and DoD missions have to work, and work well in such an environment.

The second DoD cybersecurity goal is to enable rapid and safe data sharing with any partner a mission requires that is sufficiently rich that mission execution is effective. Almost every DoD mission includes partners from outside the Department; many current solutions to satisfy cybersecurity requirements make it difficult or impossible to timely share mission data.

The third goal is that we still need to be able to protect our sensitive and classified information.

The fourth goal is to protect mission commanders' access to cyberspace. The large, shared infrastructures that DoD uses often let the mission risk assumed by one commander spill into the missions of other commanders. Our network consolidation efforts described above are designed

so that risk can be better managed so that DoD can support multiple missions, with multiple (changing) risk postures, simultaneously.

The final major DoD cybersecurity goal is that technology uptake in DoD is agile. Security requirements and processes are often cited as the reason particular technologies cannot be fielded, or are slow to be fielded. We are focused both on changing processes to better enable agile technology uptake, and on deploying technologies that can lower the risk in our use of new and/or poorly understood technologies.

Given the complexity of the cybersecurity problem, and of DoD's information technology environment, we have a wide range of technical and operational efforts aimed at achieving these goals. To achieve the dependability and secrecy goals, we have efforts to remove vulnerability, to shield latent vulnerabilities by laying defenses, and to ensure we know where vulnerabilities still exist. In spite of our best efforts to harden our systems, an adversary may still succeed, so we also have a variety of efforts to detect, diagnose, and react to successful or partially successful cyber intrusions.

An example of one of our Department-wide hardening projects is our effort to configure every DoD computer securely, keep each configured securely as new vulnerabilities are discovered, and ensure the right people know how the computer is configured. To help make this possible, this year we acquired a commercial tool we call the Assured Compliance Assessment Solution (ACAS) that all DoD Components will use to scan for configuration vulnerabilities, then report and fix these. The tool is currently undergoing final testing and will be released for deployment by this summer. Components will be deploying and operationalizating this capability over the next 18 months.

Another example, that spans the hardening, situational awareness, and cyber intrusion detection, diagnosis, and reaction areas is a modular system used throughout the department called the Host-Based Security System, or HBSS. The Department has currently deployed HBSS onto every DoD computer that connects to the unclassified or secret networks. This tool can sense and report vulnerability, shield against certain kinds of cyber intrusions, and detect and react to

others. Since it is modular, HBSS allows the DoD to deploy new hardening, situational awareness, and cyber intrusion detection, diagnosis, and reaction capabilities relatively easily by using the already-deployed HBSS software and management system. Among the cybersecurity funding requested in FY13 are funds to continue deployment and sustainment of new HBSS capability modules to better harden, to provide an automated capability to continually monitor the computer's configuration, and to improve human and device identity management capabilities across the Department.

Finally, starting this year and deploying for the next several, we have an effort to collect information from both ACAS and HBSS about the state of every DoD computer's configuration, and to use this to automatically generate mission risk scores that can be used by commanders at every level. Commanders can use this both to fix the vulnerability, and to better understand where particular missions have vulnerability. The effort is called continuous monitoring, and is being piloted in several places in DoD now. We expect to begin rolling the capability out operationally later this year.

Another key part of hardening is our effort to drive anonymity out of the networks. I discussed the DoD's deployment of Public Key Infrastructure (PKI) identity credentials on the unclassified networks earlier. This calendar year we will complete the issuance of PKI credentials to every one of the 500,000 people who use the Department's Secret network, and by March of next year we will require the use of these credentials. This will not only help us improve accountability for information access, but as we work with the rest of the Government to deploy such credentials across the Federal government will make interagency sharing safer and easier.

I would also like to point out progress and priorities in several other cybersecurity initiatives. Rapid uptake of advanced commercial technology remains a key DoD advantage. While globally sourced technology provides innumerable benefits to the Department, it also provides foreign sources with increased opportunity to compromise the supply chain by inserting malware into technology in order to access or alter data, and intercept or deny communications. In response to these risks, DoD is in the process of institutionalizing the Trusted Defense Systems / Supply Chain Risk Management (SCRM) strategies described in the Report on Trusted Defense

Systems delivered to the Congress in January 2010. DoD is also partnering with other Departments and agencies to explore approaches to managing supply chain risk within critical infrastructures.

Another critical success the Department has had is the DoD's Defense Industrial Base (DIB) Cybersecurity and Information Assurance (CS/IA) Program that DoD CIO oversees. This program offers a model standard for government-industry voluntary partnerships on cybersecurity. The program offers a holistic approach to cybersecurity, to include classified threat information sharing by the government, with voluntary sharing of incident data by industry; sharing of mitigation and remediation strategies, digital forensic analysis, and cyber intrusion damage assessments. While threats cannot be eliminated, this program enhances each DIB participant's capabilities to mitigate the risk, thereby further safeguarding DoD information that resides on, or transits, DIB unclassified networks. The Department's DIB CS/IA Program was the baseline program underlying the DIB Cyber Pilot which established an information sharing construct with Commercial Service Providers to provide managed security services enhanced by government threat information to Defense Industrial Base companies. In partnership with Homeland Security, we are working together on plans make it a permanent program for the Defense Industrial Base.

My office is doing many other things to stay on top of the cyber threat, but we must stay vigilant. The Department's cryptographic equipment must be modernized. We are analyzing the full extent of the cryptographic modernization requirement this year, and will use the data to build a 20 year modernization program with the military services. We have already completed analyses of the COMSEC modernization needs for nuclear command and control and are pursuing modernization. We have made substantial progress in planning replacement of legacy cryptographic equipment in tactical radios, and we are beginning the analysis of the other deployed cryptosystems in DoD.

IT Investment Planning

Additional changes to Department processes are necessary to ensure we can keep abreast of technological advances and defend the network against emerging cybersecurity threats.

In particular, changes to the Department's three core processes (requirements, budgeting, and acquisition) are required to address the systemic conditions resulting in DoD's stove-piped IT infrastructure. My office is working closely with the office of the Deputy Chief Management Officer on efforts to develop a flexible, agile acquisition process that also addresses the DoD's requirements and budgeting processes to institutionalize the agility and flexibility necessary in this rapidly evolving domain.

Workforce Development

A very important element of the Department's out-year cyber defense strategy is ensuring that the right workforce is in place. This means the workforce is properly sized, properly trained and has career paths that encourage growth and development of cyber defense and related skills (system management, cyber mission management, cyber operations, etc.). The Department's IT modernization effort includes a strong cyber defense workforce component that is an integral part of the Department's larger information technology and cyber workforce.

Spectrum

Another area for which I am responsible, which has become increasingly important to the Department's missions, consumers, and the economy of the nation is electromagnetic spectrum. The use of the electromagnetic spectrum continues to be a critical enabler of our warfighting capabilities and cyber operations. Defense leadership is cognizant and sensitive to the unprecedented spectrum demands resulting from the Department's increasing reliance on spectrum-dependant technologies and the rapid modernization of commercial mobile devices. Fully recognizing the linkages between national security and economic prosperity, the Department is investing in technologies and capabilities aimed at more efficient uses and management of spectrum, and for increased interoperability with our Coalition partners and with Federal, State, and Commercial entities. I look forward to working with Congress on future spectrum legislative proposals that achieve a balance between expanding wireless and broadband capabilities for the nation and the need for access to support warfighting capabilities in support of our national security.

Conclusion

Maintaining information dominance for the warfighter is critical to our national security. The efforts I've outlined today will ensure that the Department's information capabilities provide better mission effectiveness and security, and are delivered in a manner that makes the most efficient use of financial resources. I ask that you strongly support, authorize, and fund the Department's key cybersecurity and Information Technology modernization programs. I want to thank you for your interest in our efforts and I am happy to answer any questions you may have.